Las Aventuras de

Quirquincho©



Las Aventuras de

Quirquincho©



Historia: Camilo Castro (@clsource)
Ilustraciones: Leo Quezada (@leo8bits)



02 de Abril de 2018

Las Aventuras de

Quirquincho

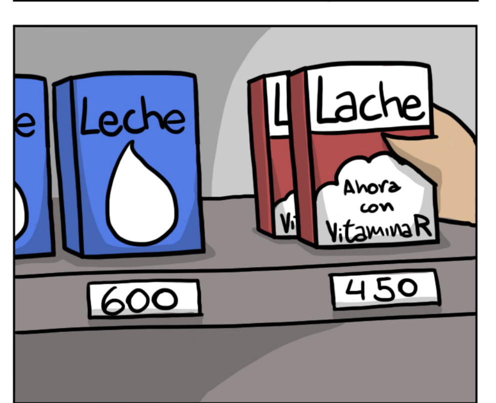
El comienzo



La historia de cómo Quirquincho se ha enamorado de las criptomonedas y el blockchain comenzó hace algunos meses.







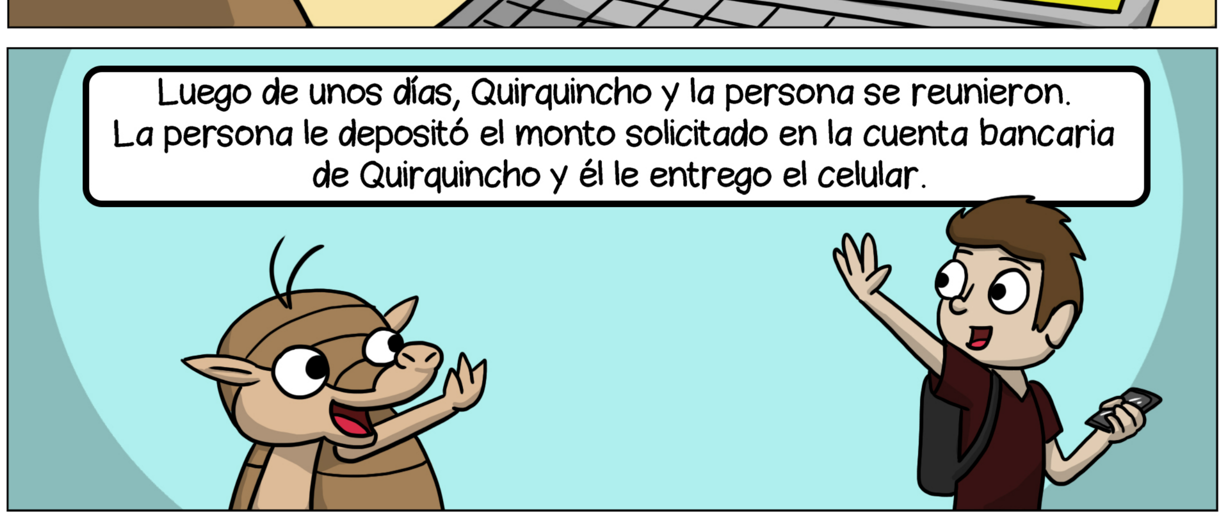


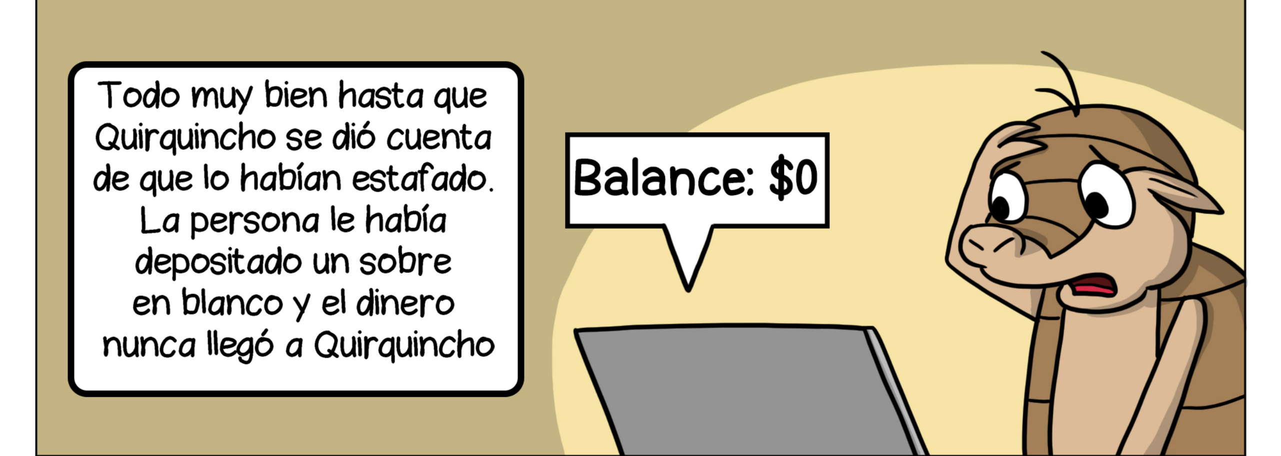
Publicó un aviso en un grupo de compra venta y al poco tiempo alguien se contactó con él.

Se vende!

Usuario

Oye me interesa

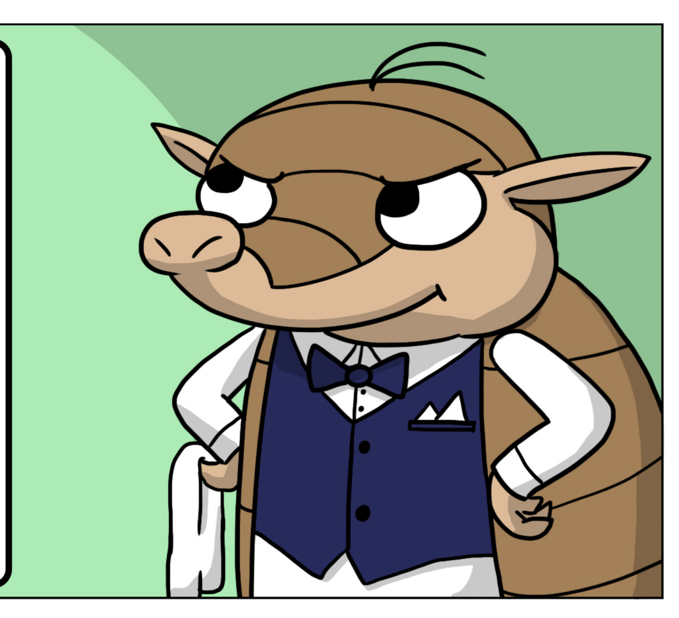




Quirquincho no pudo recuperar su celular.

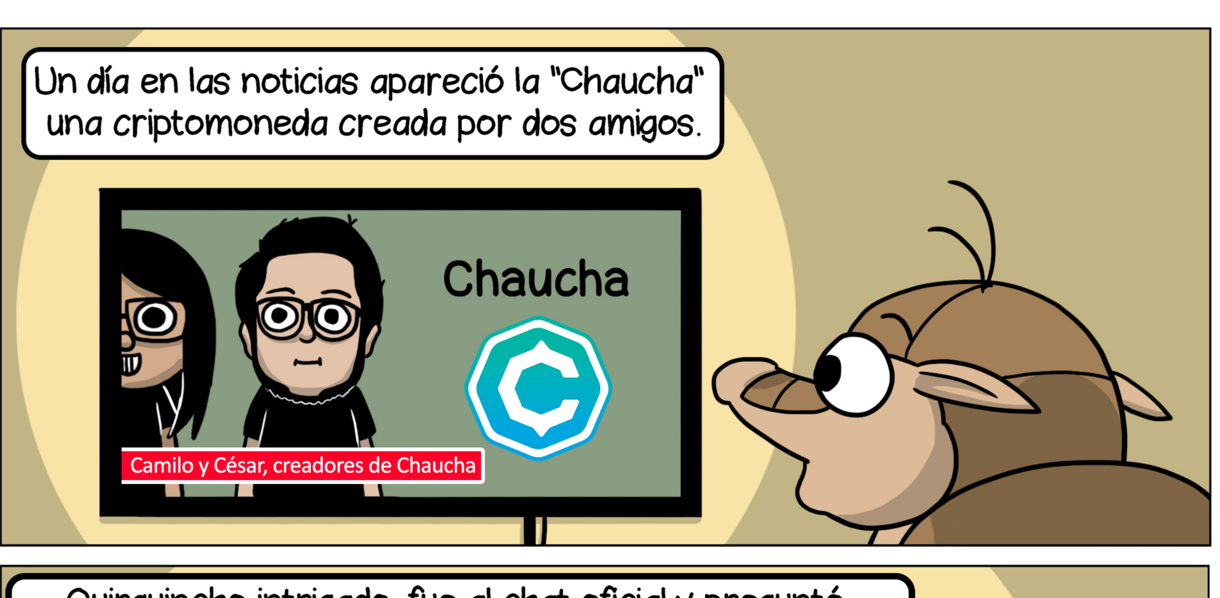
Así que decidió continuar con su objetivo de obtener el último "qPhone".

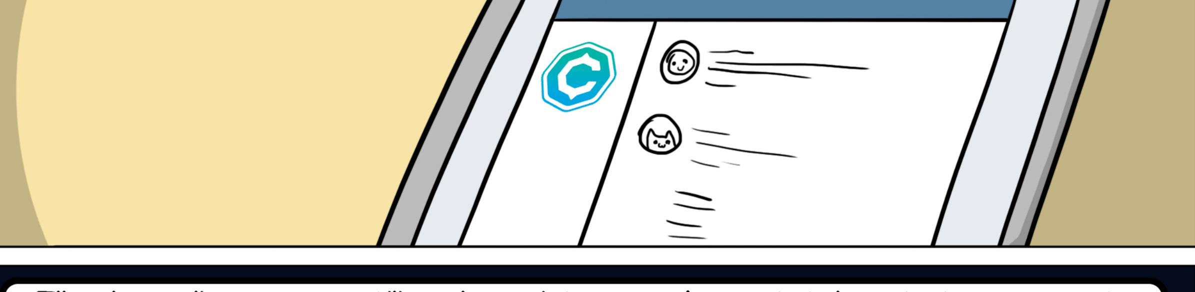
Barajando distintas alternativas, logró conseguir un empleo de garzón en un restaurante los fines de semana.

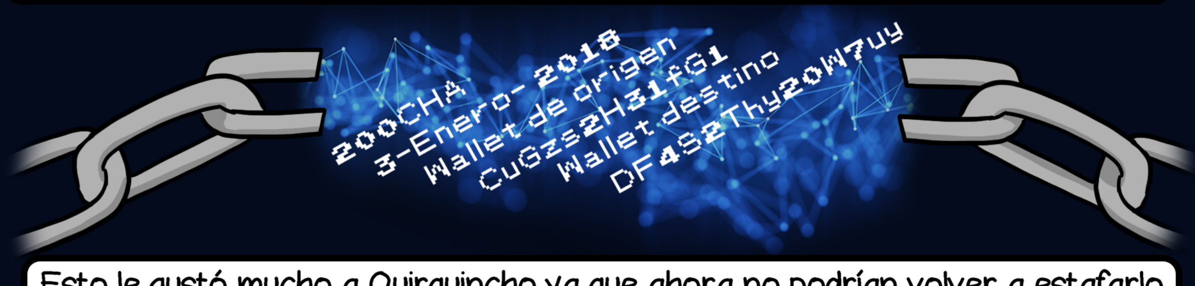


Luego de unas semanas atendiendo a los clientes, sucedieron algunos eventos que le llamaron la atención. Un día la policía llevo arrestados a la cajera y a un garzón del restaurant. Según le contaron, ellos estaban involucrados en una operación de clonación de tarjetas y dinero falsificado.

Estos eventos llevaron a Quirquincho a preguntar si existía una forma más segura de comprar y vender.


Un día en las noticias apareció la "Chaucha" una criptomoneda creada por dos amigos.
Chaucha
Camilo y César, creadores de Chaucha

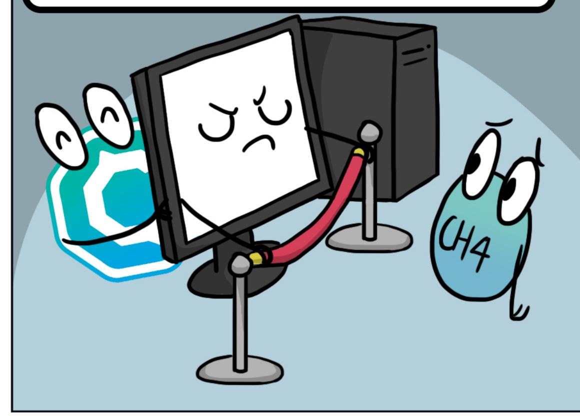

Quirquincho intrigado, fue al chat oficial y preguntó a los amigos de chaucha sobre cómo una criptomoneda es mejor que utilizar el dinero tradicional.


Ellos le explicaron que utilizar las criptomonedas es totalmente transparente gracias a la tecnología del blockchain. Donde puedes verificar fácilmente si han realizado un depósito, su monto, fecha, origen y destino en poco tiempo.
Además de que no se puede modificar o eliminar la información una vez ingresada a la red.
200CHA
3-Enero-2018
Wallet de origen
CuGzs2H31fG1
Wallet destino
DF4S2Thy20W7uy
Esto le gustó mucho a Quirquincho ya que ahora no podrían volver a estafarlo con depósitos sin fondo o con información poco clara.

Además le explicaron que crear criptomonedas falsas o inexistentes no es posible debido a que la red rechazaría tales monedas al tener características distintas a las que se consideran legítimas.



Como las computadoras son muy buenas en cálculos matemáticos pueden diferenciar fácilmente una moneda legítima de una falsa.



Quirquincho quedó muy contento al saber que no habría posibilidad de recibir chauchas falsificadas.

También les preguntó sobre la posibilidad de clonación de tarjetas. Los amigos de chaucha le explicaron que toda cadena es tan fuerte como su eslabón más débil.



Esto quiere decir que existe la posibilidad de que te roben tus chauchas, sin embargo, esto es mayoritariamente debido a descuidos personales.



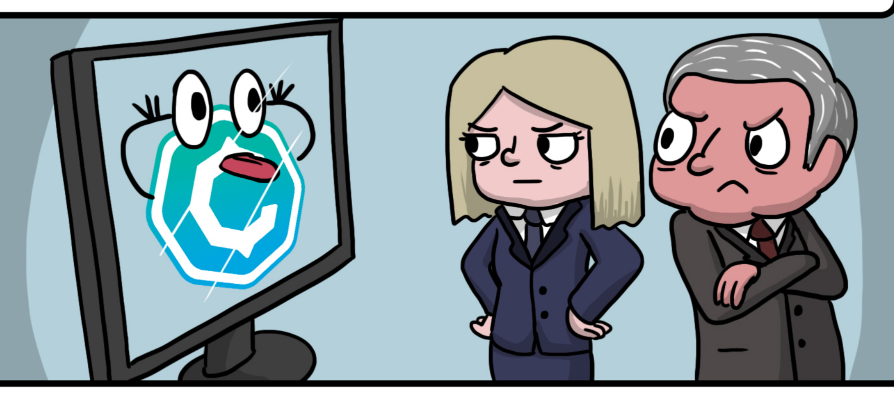
Las criptomonedas tienen la ventaja de tener múltiples métodos para resguardarlas de robos y accidentes. Como por ejemplo crear "chaucheras" de papel y ocultarlas.

Además de contar con altos niveles de seguridad que hacen prácticamente imposible que alguien "adivine" la llave privada que autoriza el uso de tus chauchas.



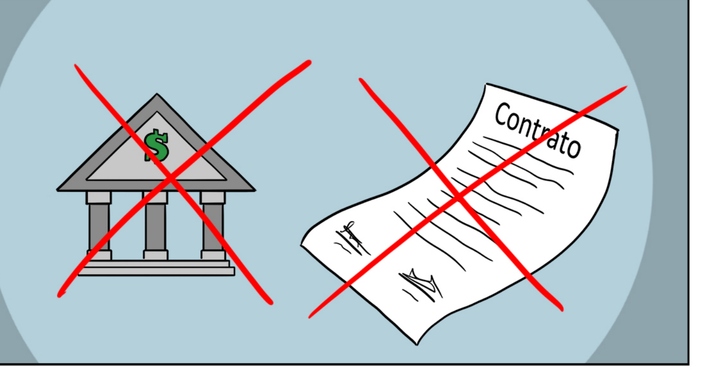


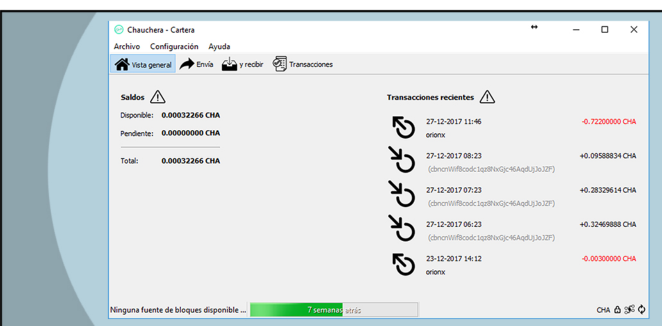
Otra característica es que la red chaucha no puede ser censurada por un gobierno o entidad poderosa.



Es decir que no la pueden "eliminar" debido a que la red funciona con miles de computadoras distribuidas por el mundo.

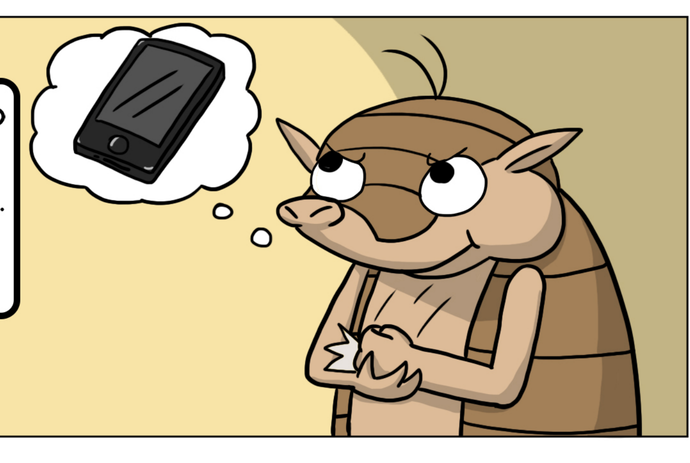
La característica que más le gustó a Quirquincho es que no necesitas tener un banco para poder utilizar las criptomonedas. No hay que tener un contrato o pagar algún tipo de mensualidades a nadie.

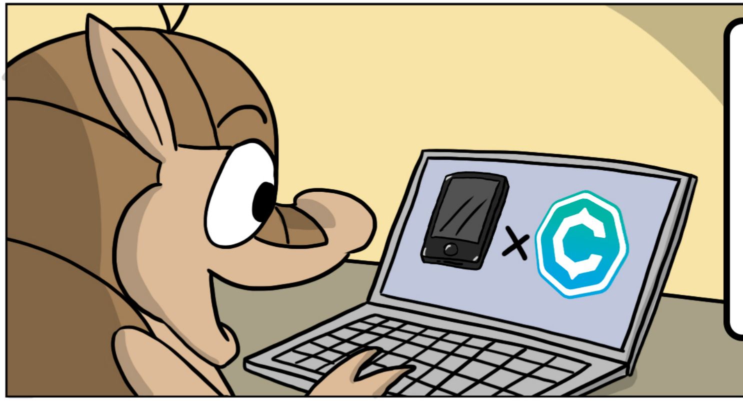




Quirquincho ahora no necesitaba dar datos personales para recibir y hacer depósitos. Gracias a que la red de chaucha es totalmente anónima.

Quirquincho quedó muy contento y decidió aprender más sobre el tema y compartirlo con todos. Pero primero necesitaba comprar el "qPhone".





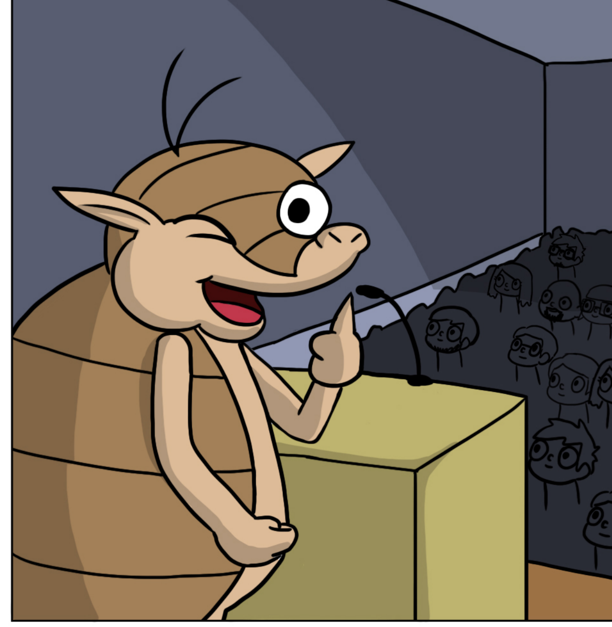
Un amigo puso a la venta un "qPhone" de última generación a cambio de chauchas y Quirquincho, que había ahorrado lo suficiente lo compró casi al instante.

El proceso fue rápido y transparente, Quirquincho se reunió con el amigo, depositó las chauchas solicitadas y por fin obtuvo su "qPhone".



Ahora Quirquincho se dedica a explicar sobre las criptomonedas y cómo la tecnología blockchain puede cambiar nuestra sociedad de la misma forma que lo hizo internet.



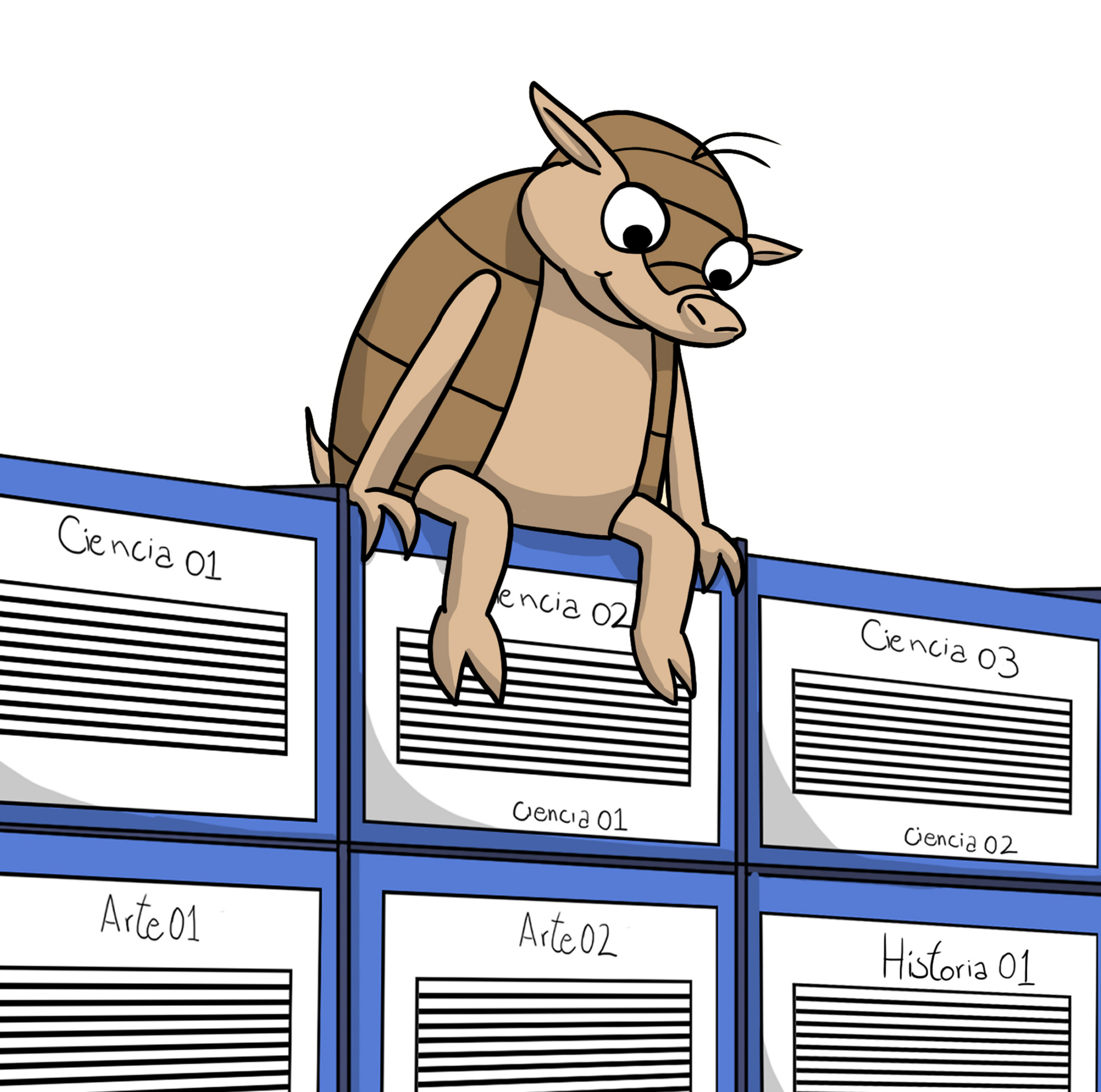


Quirquincho continuará enseñandonos sobre la tecnología del Blockchain

Las Aventuras de

Quirquincho

Blockchain



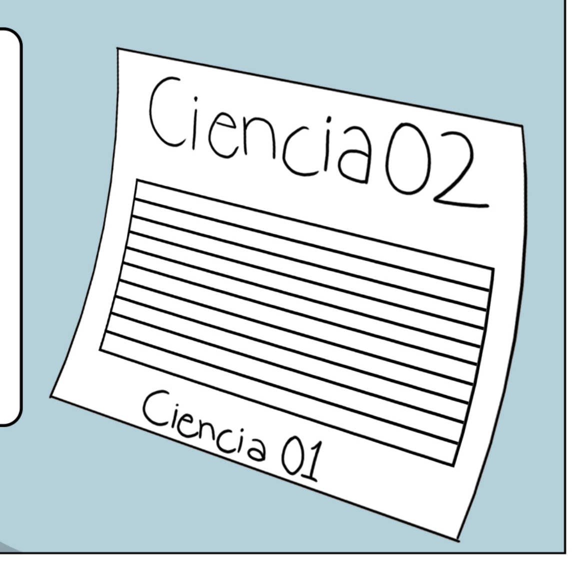


Un día se dió cuenta de que estaba muy desordenada. Entonces decidió cambiar los muebles y crear una mejor forma de organizarlos.

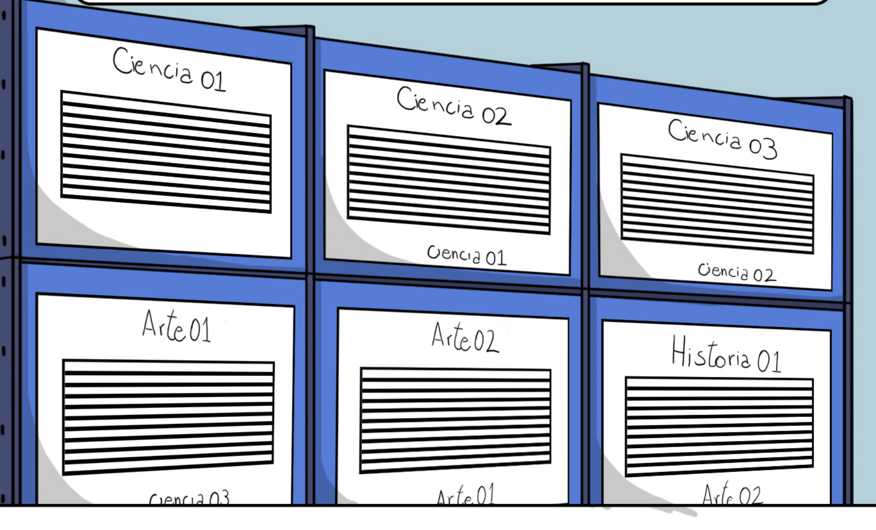


El primer identificador contenía la categoría de la caja y su número único. Por ejemplo, Ciencia 02.

El segundo identificador contenía el identificador (categoría y número) de la caja anterior.

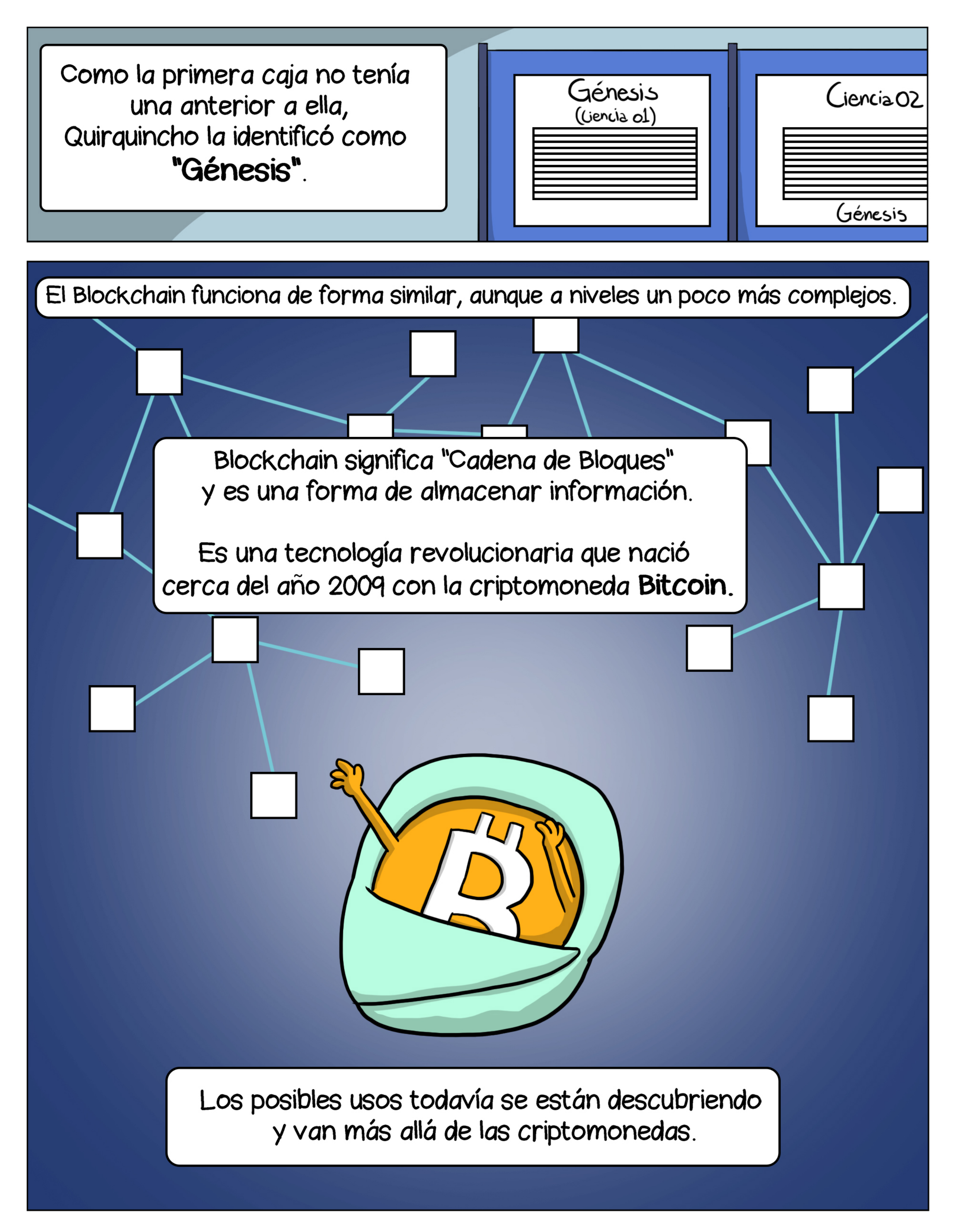


Finalmente pegó una hoja en cada caja. Esta hoja tenía un listado de 10 libros que debían ser almacenados en aquella caja.



De esta forma Quirquincho podía saber exactamente el orden de cada caja y los libros que debían contener.

Si algún día se cambia de casa, sería fácil volver a ordenar los libros de la misma forma.


Como la primera caja no tenía una anterior a ella, Quirquincho la identificó como **"Génesis"**.
Génesis
(Ciencia 01)
Ciencia 02
Génesis
El Blockchain funciona de forma similar, aunque a niveles un poco más complejos.
Blockchain significa "Cadena de Bloques" y es una forma de almacenar información.
Es una tecnología revolucionaria que nació cerca del año 2009 con la criptomoneda **Bitcoin**.
Los posibles usos todavía se están descubriendo y van más allá de las criptomonedas.


Al igual que las cajas que elaboró Quirquincho,
el Blockchain utiliza bloques para almacenar datos.
Cada bloque tiene un tamaño máximo
y dos identificadores para poder organizarlos.
Génesis
Gracias a estos identificadores es posible saber exactamente la posición
del bloque y navegar por la cadena hasta el bloque **"Génesis"**.
Estos identificadores son generados automáticamente
dependiendo del contenido que tenga el bloque.
Usar la tecnología de Blockchain tiene
la ventaja de que si alguien altera la información
de un bloque ya incluido en la cadena,
los identificadores de ese bloque cambiarán.
Lo que obligaría a rehacer la cadena
completamente. Un proceso muy costoso
y mientras más bloques más difícil es.

Esto abre las puertas a novedosas formas de almacenar datos y asegurar de que estos son confiables.



Las criptomonedas como Chaucha, utilizan la tecnología del Blockchain para guardar información de las transacciones.

Es un gran libro contable compartido por todos de forma pública.

Puedes saber cuantas chauchas tiene una dirección, de dónde las obtuvo y a dónde las ha enviado.

Aunque no se puede saber quien es el dueño de esa dirección.

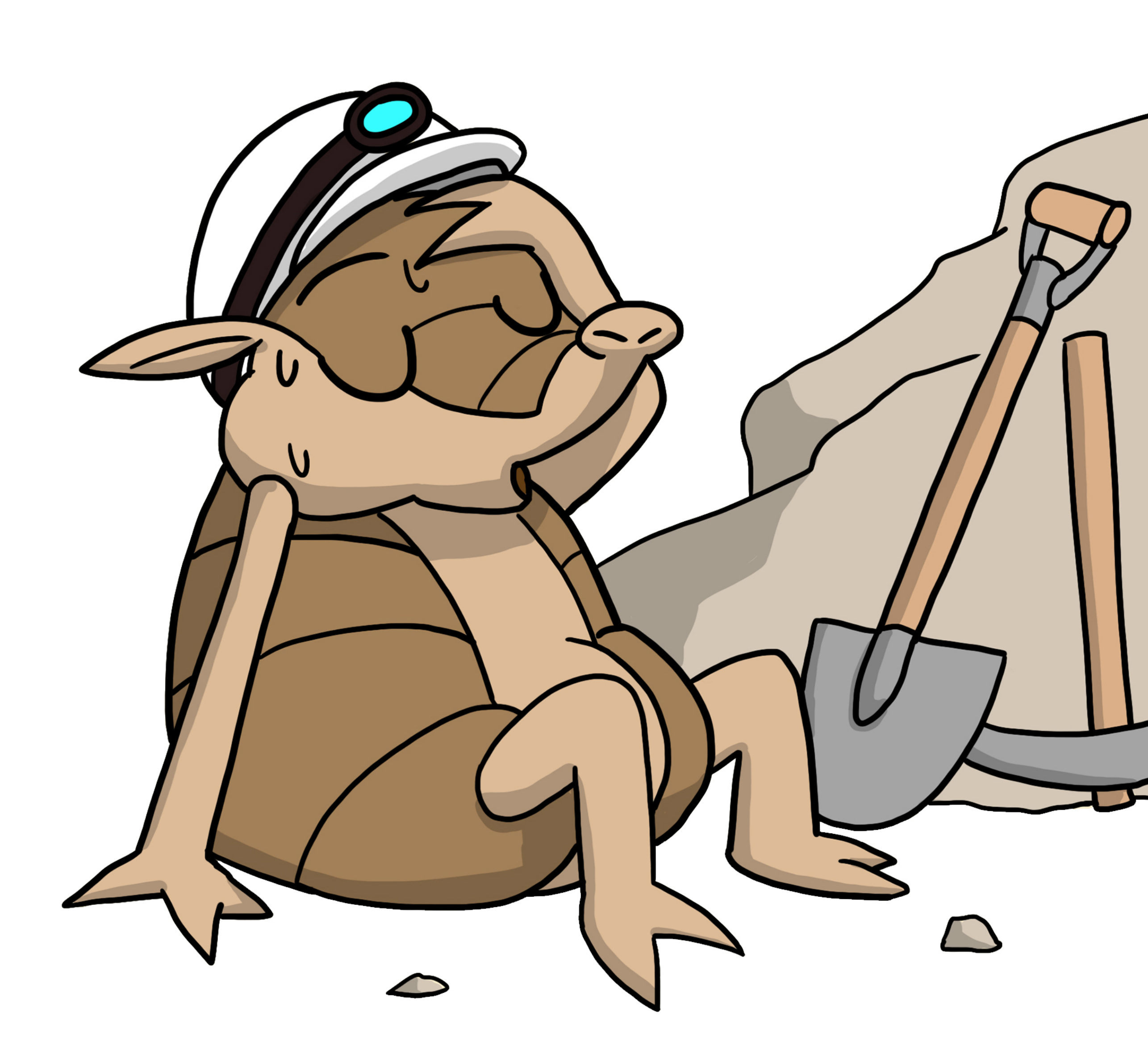


A contiucación, Quirquincho nos explicará el rol de los Mineros

Las Aventuras de

Quirquincho

Mineros



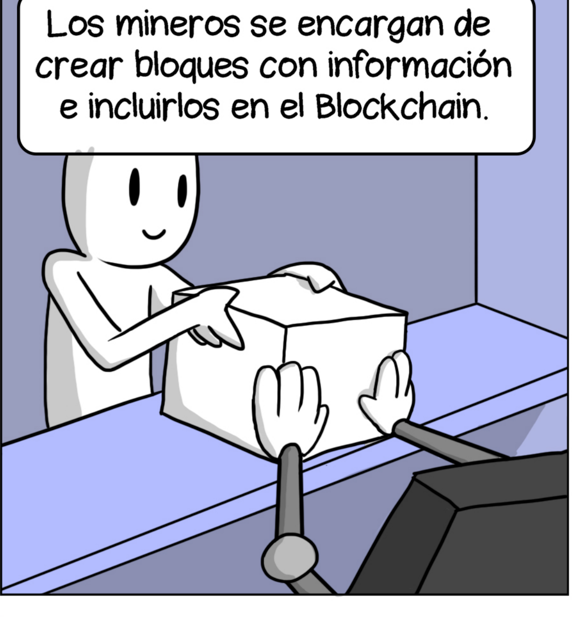




Al pasar los años, muchas personas comenzaron a llegar con máquinas más complejas y poderosas.

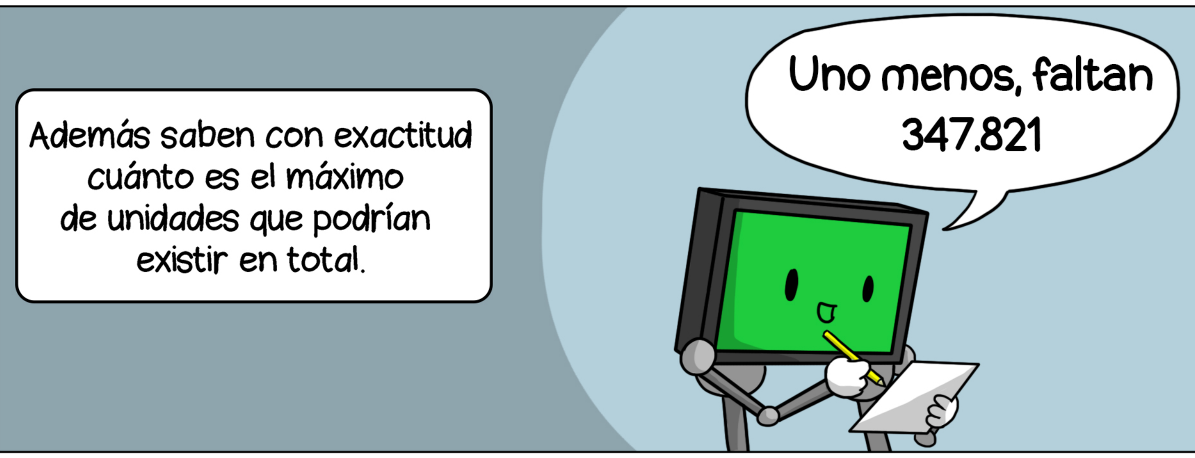
Esto causó de que hoy conseguir oro sea algo muy difícil. Ya que requiere de gran inversión de tiempo y esfuerzo.



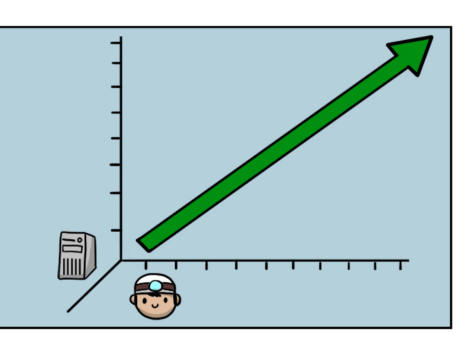


Cada vez que logran ingresar un bloque en el Blockchain, los mineros obtienen un premio en la criptomoneda minada.

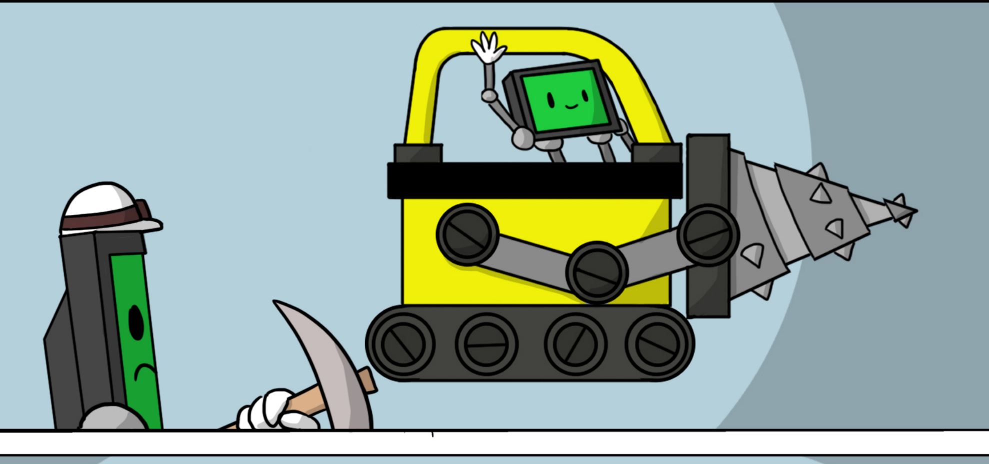
BlockChain



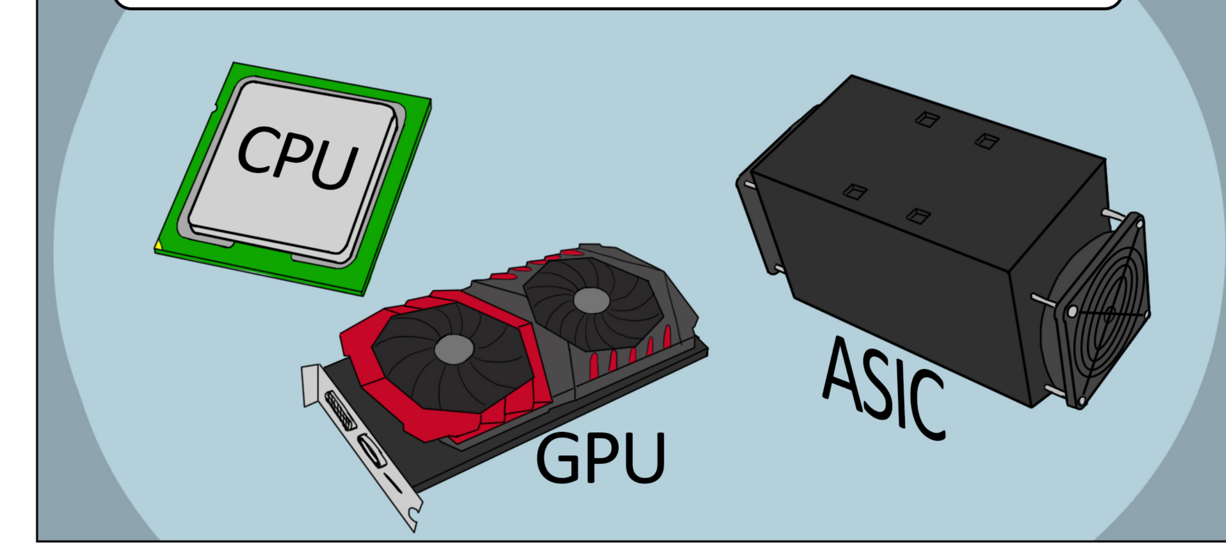
En Chaucha al igual que la minería tradicional, mientras más mineros ingresen a la red, más capacidad de procesamiento necesitan.



Es decir, más difícil es ingresar un bloque y obtener chauchas. Lo que los obliga a utilizar herramientas cada vez más potentes.



Las herramientas de los mineros son diversas y su efectividad depende de la criptomoneda y sus reglas.

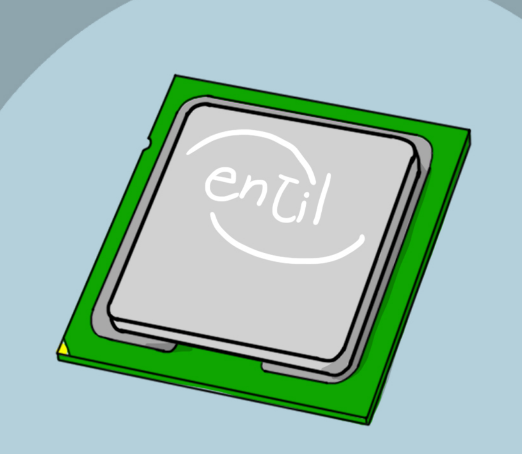


Entre las posibles opciones tenemos:

CPU

Central Processing Unit
Unidad de Central de Procesamiento

Presente en las computadoras tradicionales.
Usados para ejecutar las operaciones normales de un computador

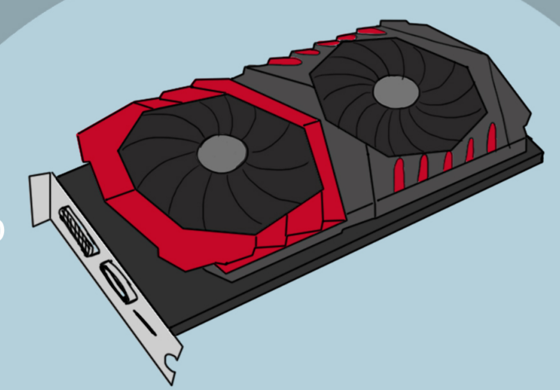


Costo de Adquisición: Bajo - Medio
Poder de Procesamiento: Bajo
Consumo de Energía: Bajo

GPU

Graphic Processing Unit
Unidad de Procesamiento Gráfico

Son las tarjetas gráficas de los computadores.
Normalmente utilizadas para aplicaciones audiovisuales como videojuegos



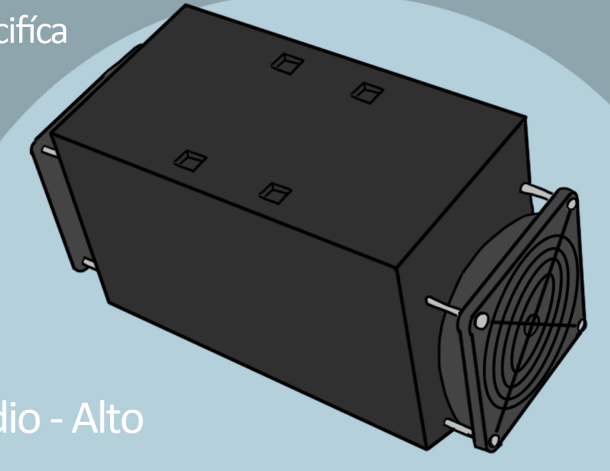
Costo de Adquisición: Medio - Alto
Poder de Procesamiento: Medio
Consumo de Energía: Medio

ASIC

Aplication-Specific Integrated Circuit

Circuito integrado de aplicación especifíca

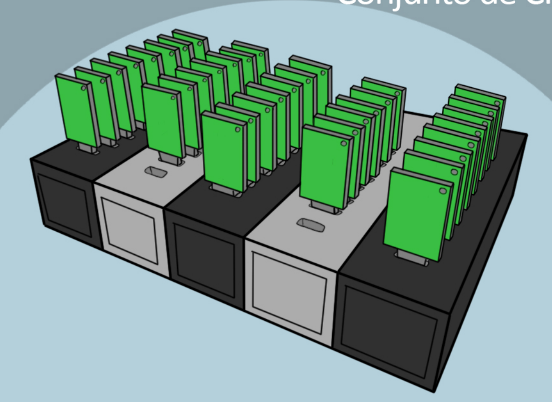
Son equipos especialmente creados con el fin de cumplir una tarea específica. Comúnmente se usan para minar criptomonedas.



Costo de Adquisición: Alto
Poder de Procesamiento: Medio - Alto
Consumo de Energía: Alto

CPU/GPU/ASIC RIG

Conjunto de CPU/GPU/ASIC



Son varias CPU, GPU o ASIC que trabajan de forma unificada colaborando entre sí para obtener un mayor poder de procesamiento

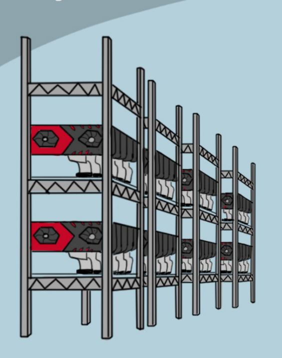
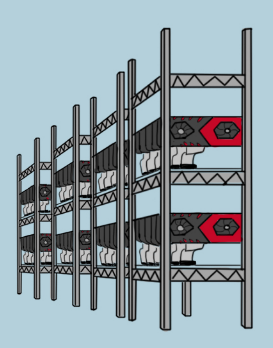
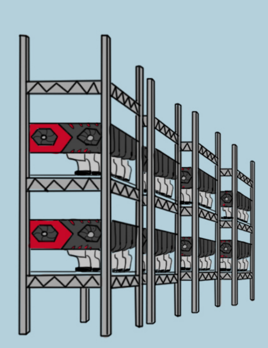
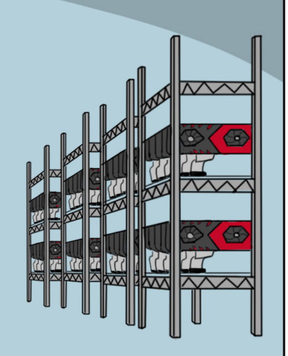
Costo de Adquisición: Medio - Alto
Poder de Procesamiento: Medio - Alto
Consumo de Energía: Medio - Alto

Cloud Mining

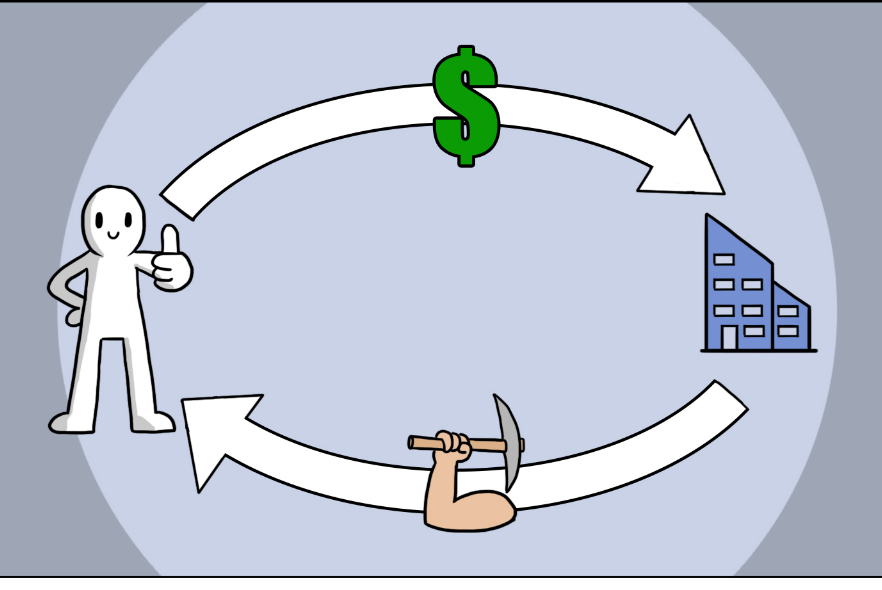
Minería en la Nube

Existen empresas que tienen a su disposición “Granjas de Minería”. Estas “Granjas” son uno o más conjuntos de CPU/GPU/ASIC (RIG)

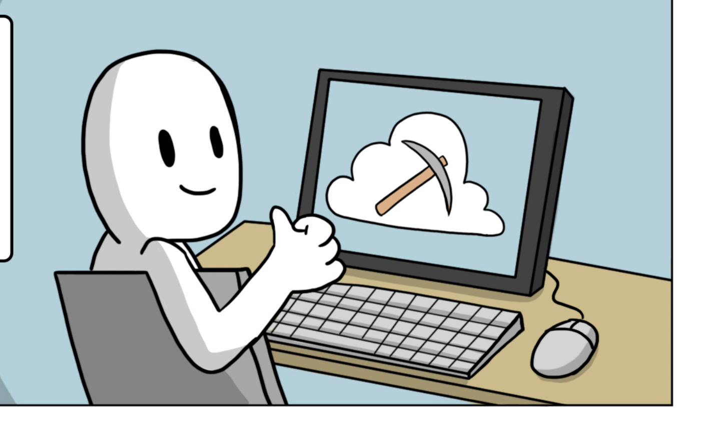
Estas empresas arriendan poder de procesamiento.

Las personas pueden obtener este poder de minería pagando lo que solicite la empresa por un tiempo determinado.



De esta forma las personas pueden minar la criptomoneda que más deseen sin tener que invertir costosas sumas en máquinas o energía.



Una herramienta importante son las "Pools" (Piscinas).

Pool

Son servidores donde varios mineros se reúnen y comparten su poder de procesamiento

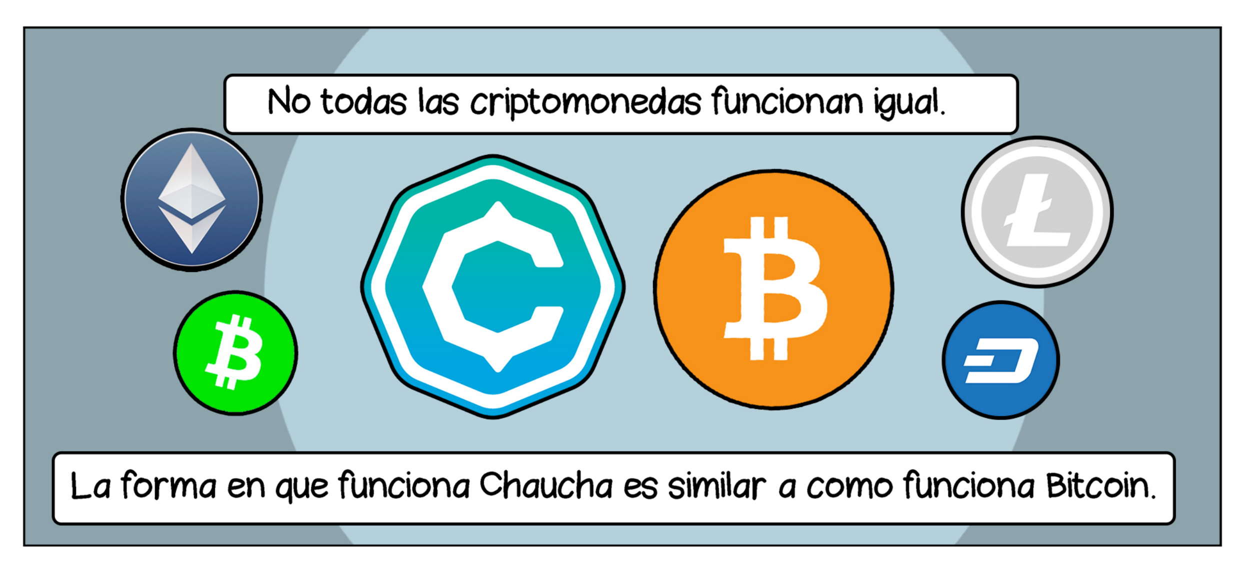
Cuando logran ingresar un bloque al Blockchain,
se reparte el premio entre todos dependiendo
del poder de procesamiento que han aportado.

Una "Pool" se puede considerar como una
gran "Granja Minera" distribuida en varios mineros.

Imaginen un conductor que necesita
empujar su automóvil para hacerlo andar.

Le ofrece a tres personas (una fuerte y dos normales),
pagar el porcentaje de una unidad dependiendo
de la fuerza que ellos han aportado al empujar.

Cuando el vehículo logra partir,
el conductor le paga 0.8 al más fuerte
y 0.1 a las otras dos personas.



Quirquincho nos explicará lo que es "Proof of Work"

Las Aventuras de

Quirquincho

Proof of Work

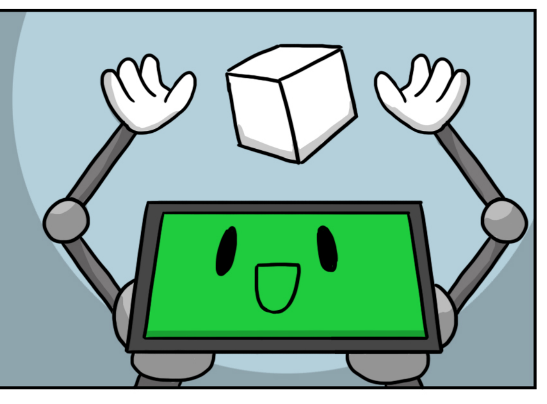


El pirquinero le pidió ayuda a Quirquincho a llevar sus capachos.

Hicieron una pequeña carrera hacia la ciudad y el pirquinero le regaló un recuerdo de Andacollo a Quirquincho por su buena onda.



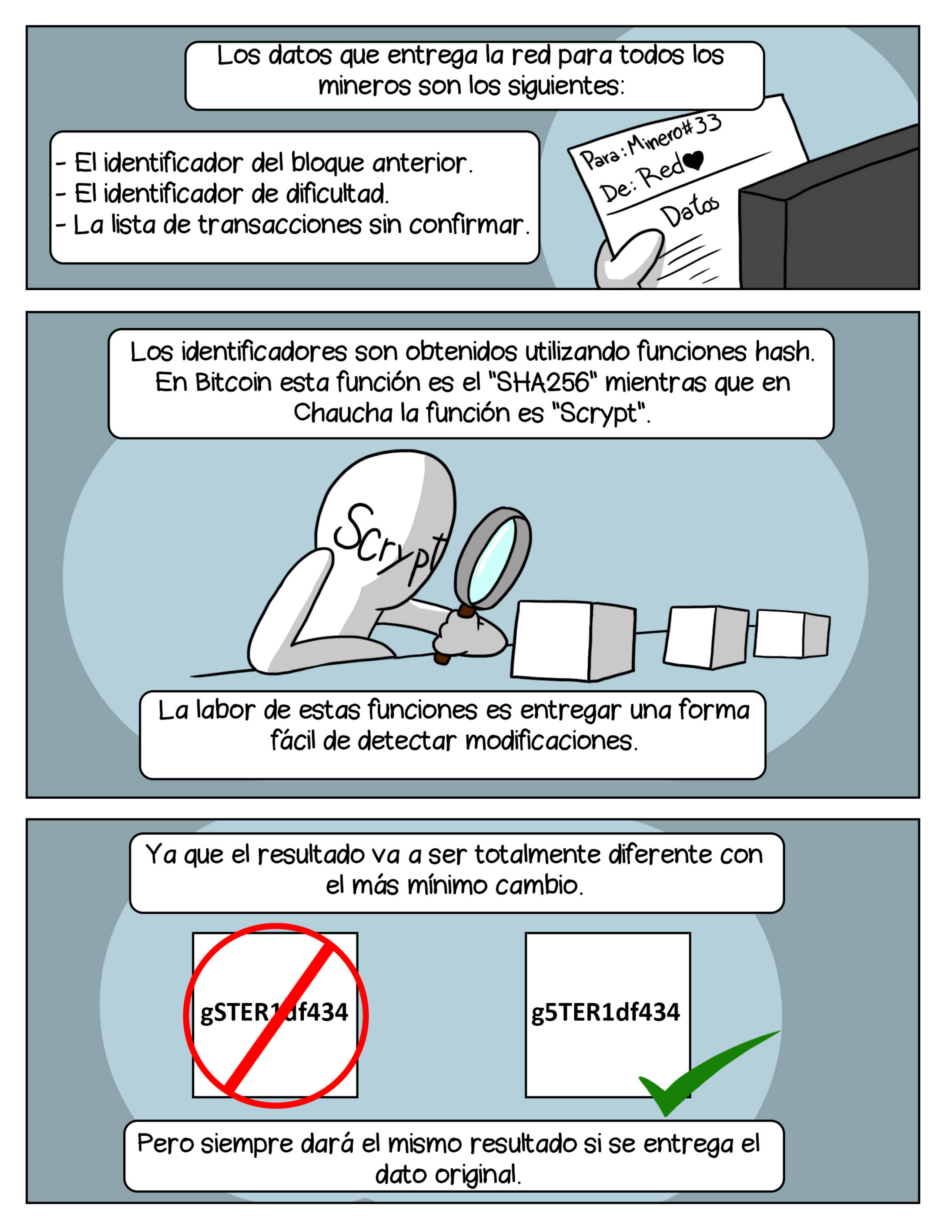






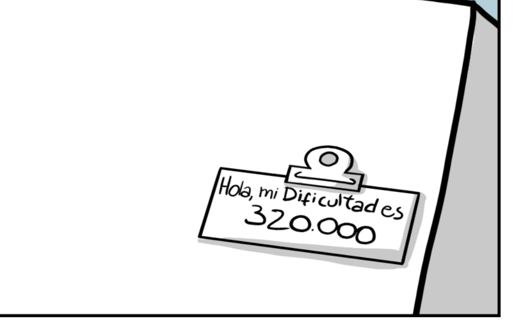
En ese momento todos los mineros desechan el bloque que estaban haciendo y comienzan a crear uno nuevo, utilizando los últimos datos.

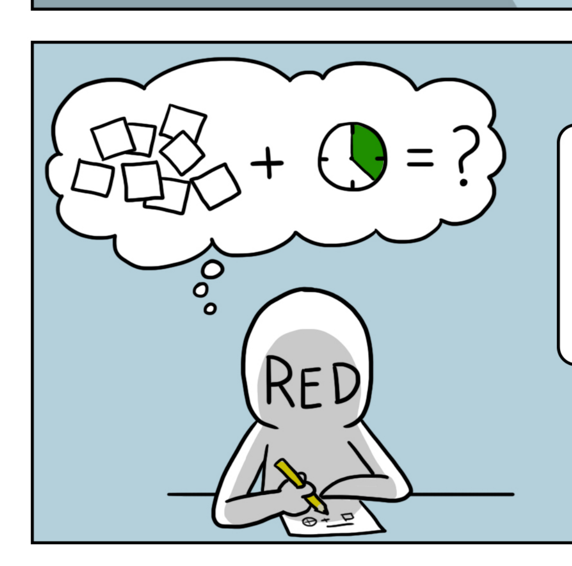
Basura



Los datos que entrega la red para todos los mineros son los siguientes:
- El identificador del bloque anterior.
- El identificador de dificultad.
- La lista de transacciones sin confirmar.
Para: Minero#33
De: Red
Datos
Los identificadores son obtenidos utilizando funciones hash. En Bitcoin esta función es el "SHA256" mientras que en Chaucha la función es "Scrypt".
Scrypt
La labor de estas funciones es entregar una forma fácil de detectar modificaciones.
Ya que el resultado va a ser totalmente diferente con el más mínimo cambio.
gSTER1df434
g5TER1df434
Pero siempre dará el mismo resultado si se entrega el dato original.

El identificador de dificultad es la pieza clave que permite saber si un bloque ganó la competencia y puede ser incluido en el blockchain.



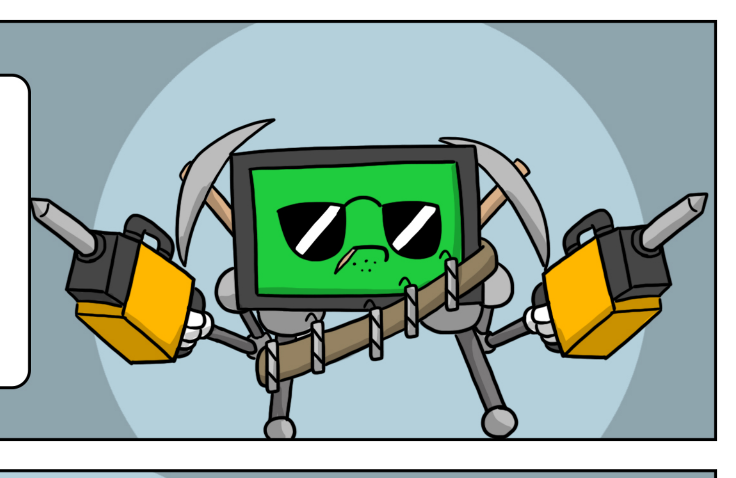


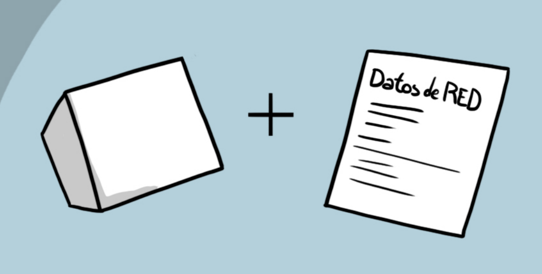
Es generado automáticamente por la red dependiendo de distintos factores como la cantidad de bloques anteriores y el tiempo en que tomaron en ser incluidos.

Puede ser un número grande o un número pequeño y variará constantemente.
Mientras más pequeño es el número de este identificador, más difícil será encontrar un número menor.

Dificultad
600
500
400
300
200
100
1 Día
2 Días
3 Días
4 Días
5 Días
6 Días
7 Días

Los mineros utilizan todo su arsenal de procesamiento para encontrar un identificador de bloque que sea menor al identificador de dificultad.

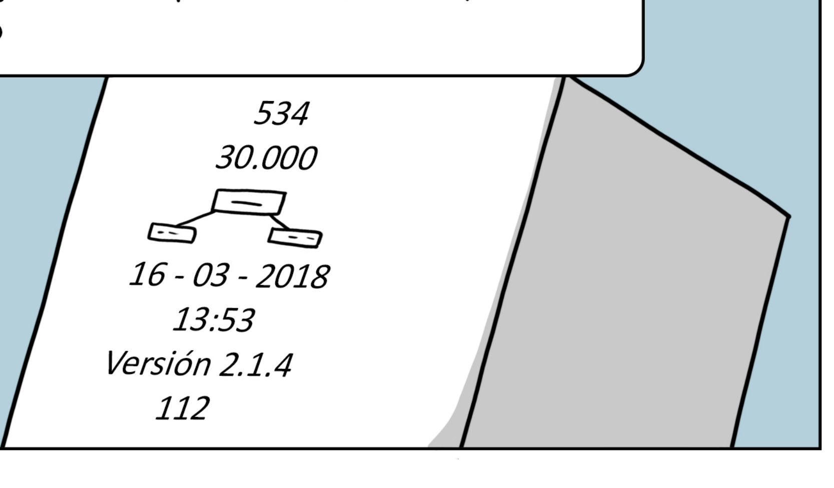




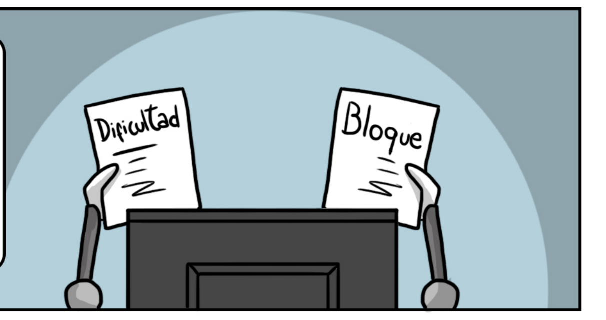
Este identificador de bloque es obtenido juntando los datos otorgados por la red con los datos propios de cada bloque.

En total un bloque tiene los siguientes datos:

- El identificador del bloque anterior
- El identificador de dificultad
- El identificador de las transacciones incluidas (Merkle Root)
- La fecha y hora de creación del bloque
- La versión de las reglas usadas para validar el bloque
- Un número aleatorio



Los mineros unen todos estos datos y aplican la función hash para obtener el identificador del bloque. Luego comparan este hash con el identificador de dificultad.



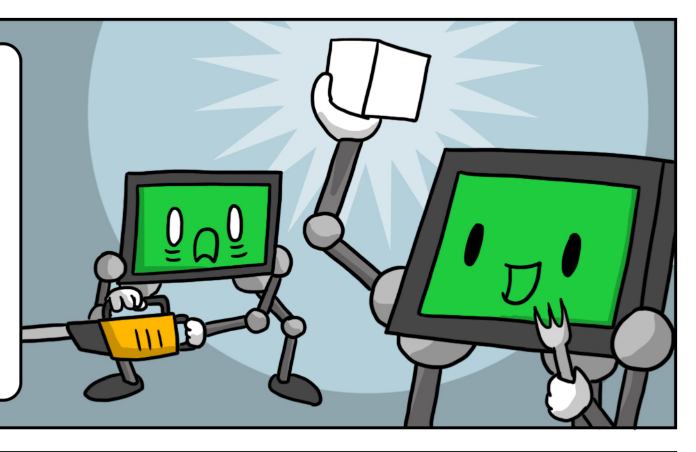
Si el valor es menor han ganado y la red anuncia que se ha incluido un nuevo bloque.

RED

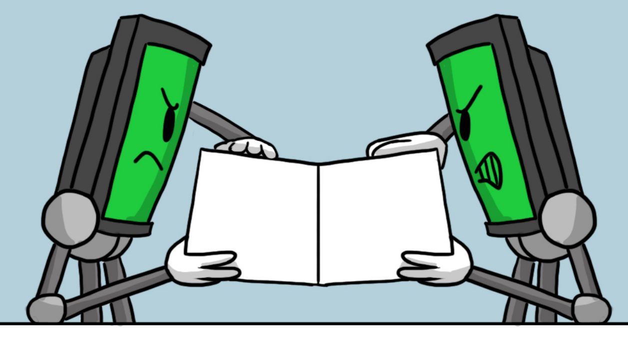
¡Hay bloque nuevo!

Este proceso toma tiempo y deben probar millones de distintas combinaciones. Variando el número aleatorio, la fecha o el identificador de transacciones.

Es en esta labor donde
ocupan casi toda la capacidad
de procesamiento.
Aunque de ves en cuando algún
minero con poca capacidad
de procesamiento igual
puede achuntarle al
identificador ganador.



En ocasiones dos o más mineros encuentran un identificador
ganador casi al mismo tiempo.
Lo que obliga a todos a decidir qué bloque debe ser
considerado como oficial.

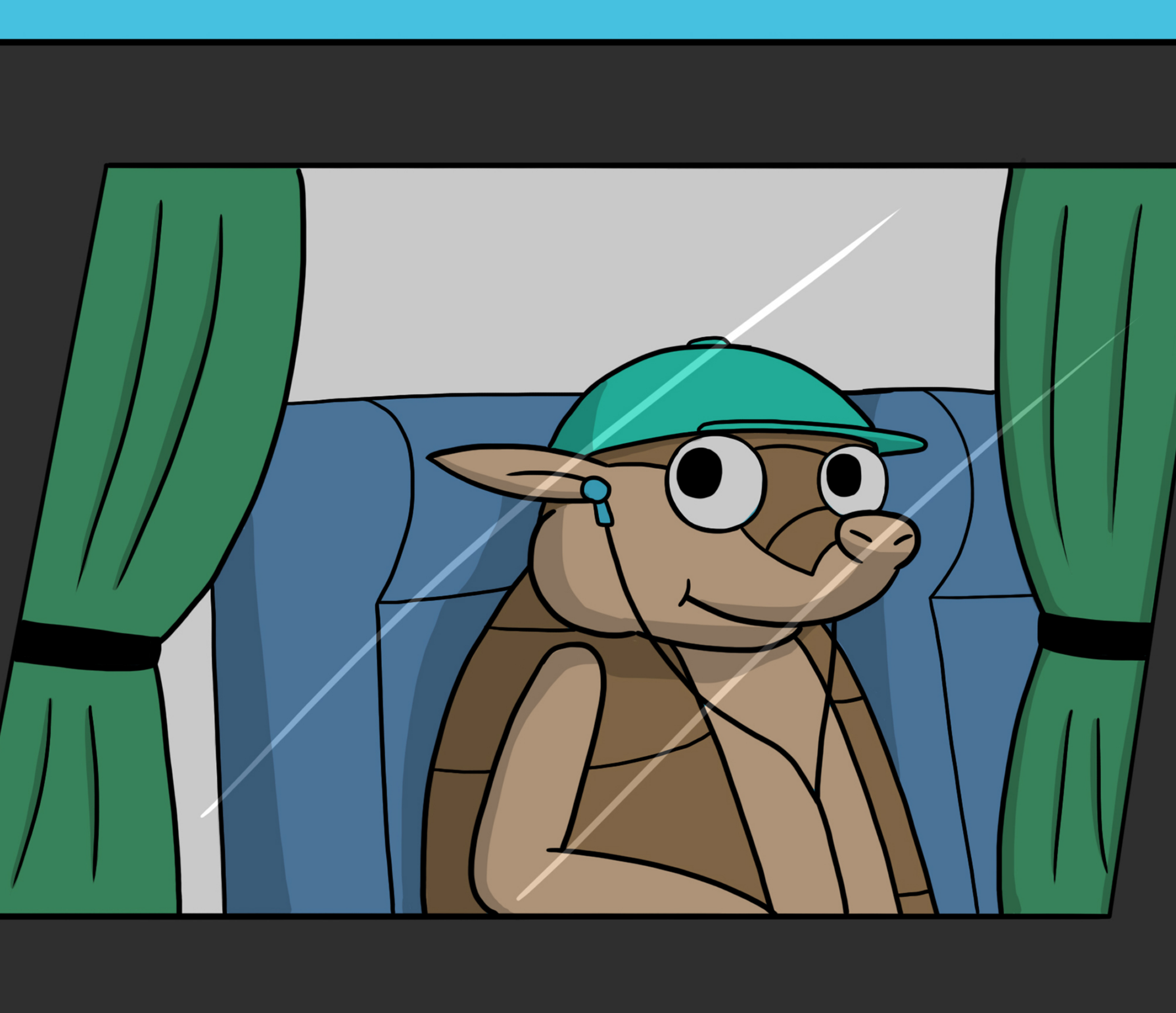




Las Aventuras de

Quirquincho

Conflictos en la red

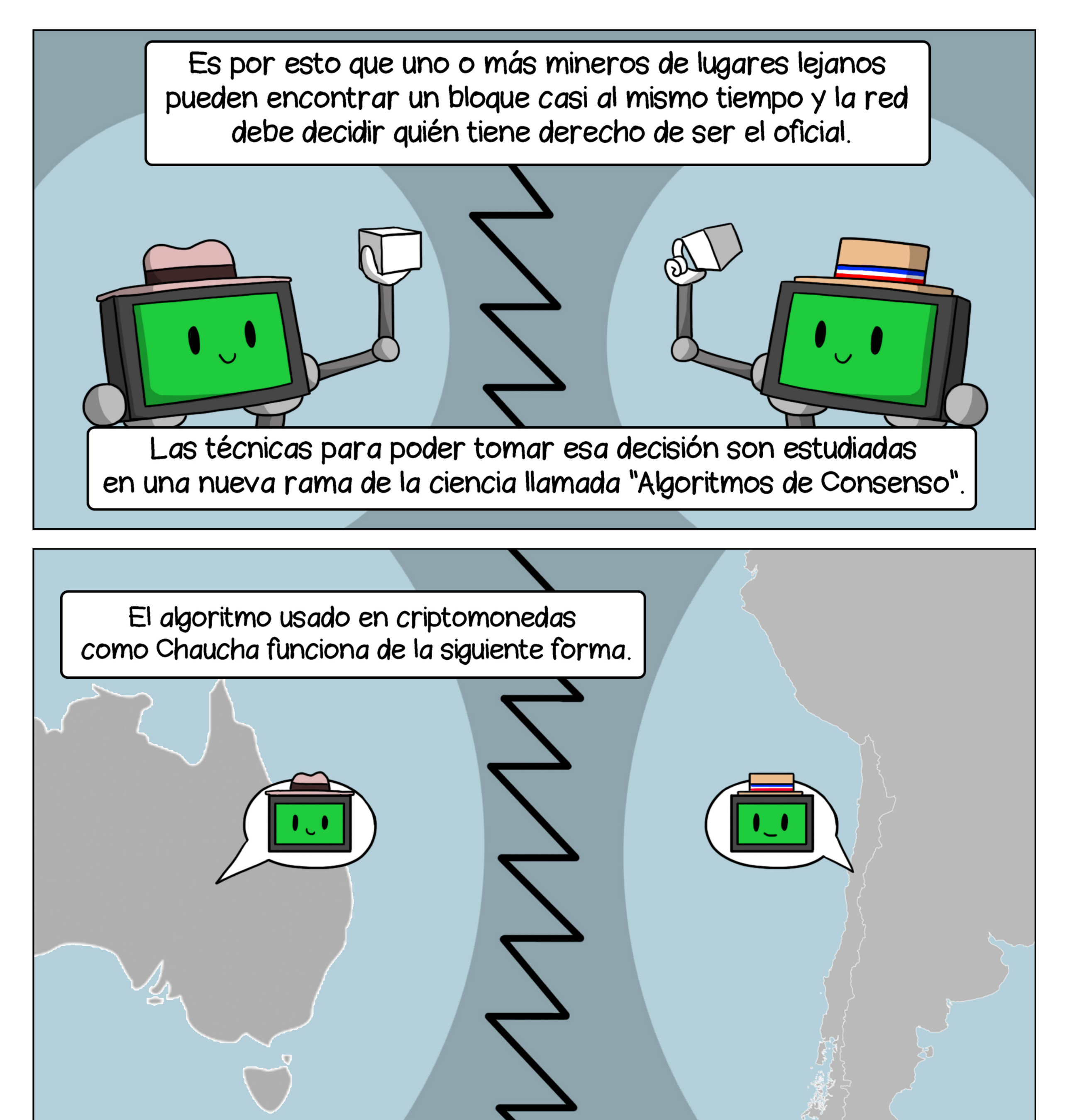


Quirquincho muy contento con su visita en Andacollo se preparó para volver a su hogar.

Se despidió de su nuevo amigo pirquinero y emprendió el viaje a casa.

Al igual que quirquincho que viajaba en un bus, la información viaja por la red hacia los mineros.



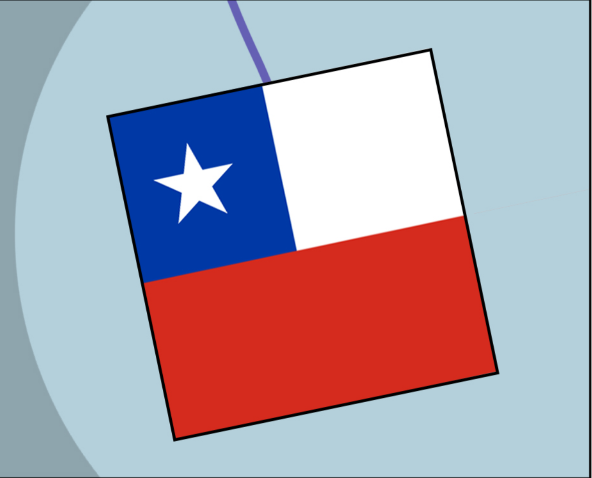


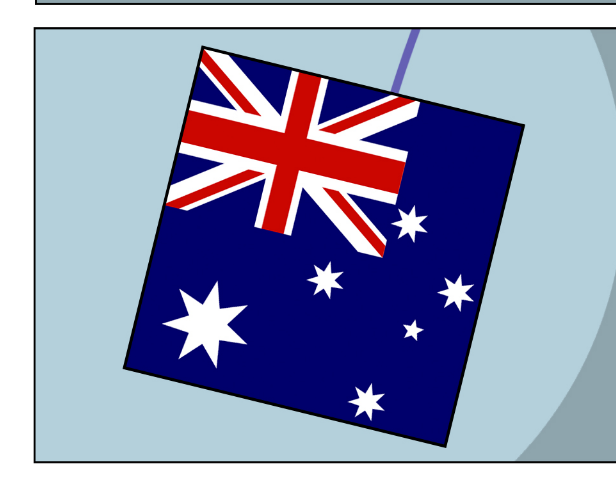
Digamos que en Chile un minero obtiene el derecho de incluir un bloque. Mientras que en Australia otro minero también gana ese derecho.

Como son sectores muy distantes entre sí, la información sobre que bloque es el ganador se distribuye de forma distinta.

La red le entrega la recompensa completa al minero de Chile y también al de Australia.

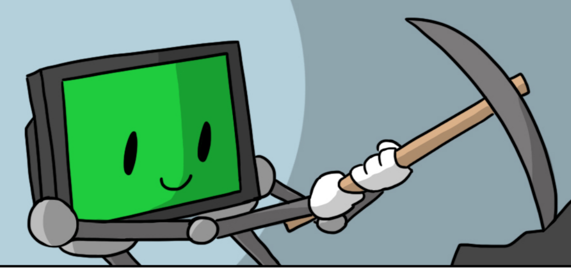
Los mineros que estén más cerca de Chile sabrán primero que el bloque ganador provino de Chile...

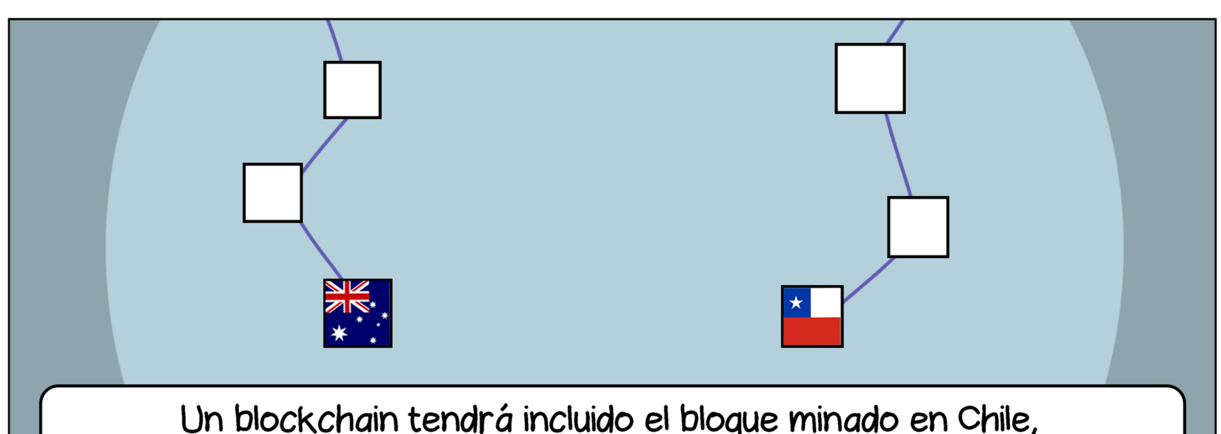




... Mientras que los mineros que estén más cerca de Australia sabrán que el bloque ganador provino de Australia.

Los mineros continúan con su labor normalmente, pero ahora existirán dos versiones distintas del blockchain.





Un blockchain tendrá incluido el bloque minado en Chile, mientras que otra versión tendrá incluido el bloque minado en Australia.

La versión oficial se define dependiendo de cúal versión del blockchain es más larga, es decir la que tenga más bloques minados.

Mientras más poder de minado, más bloques se podrán obtener y se creará un blockchain más largo de forma más rápida.

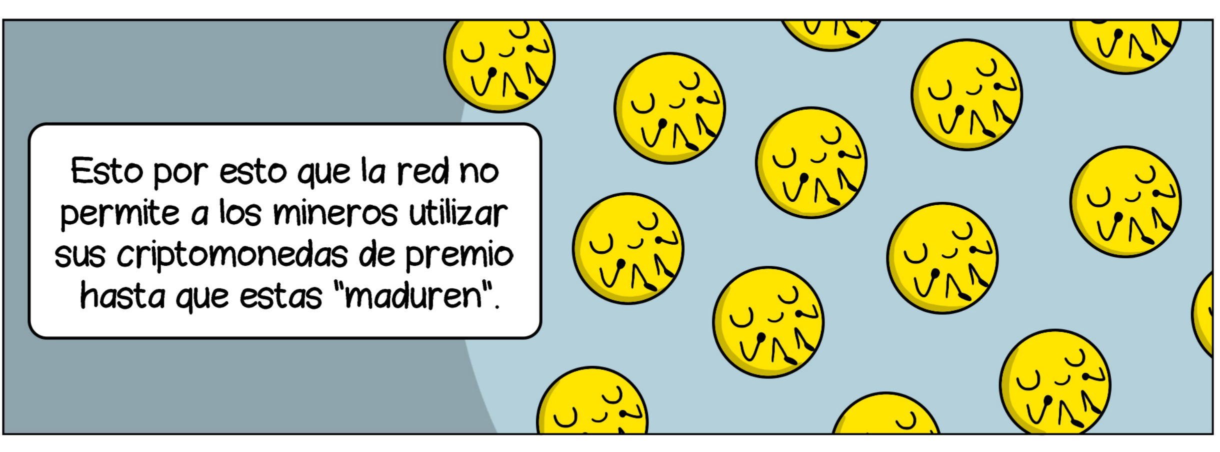
Si el sector cercano a Chile tiene más poder de minado que el sector cercano a Australia, es probable de que la versión del blockchain usada en Chile gane el derecho a convertirse en oficial.

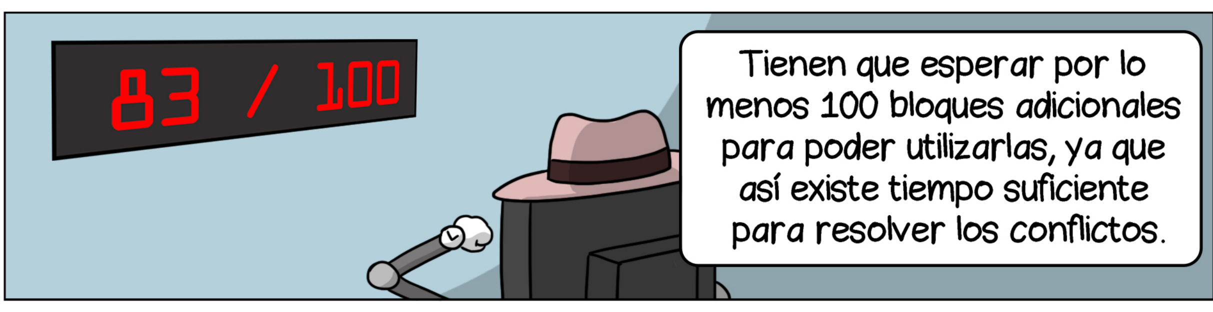
Cuando se define la versión oficial, la otra versión es desechada.

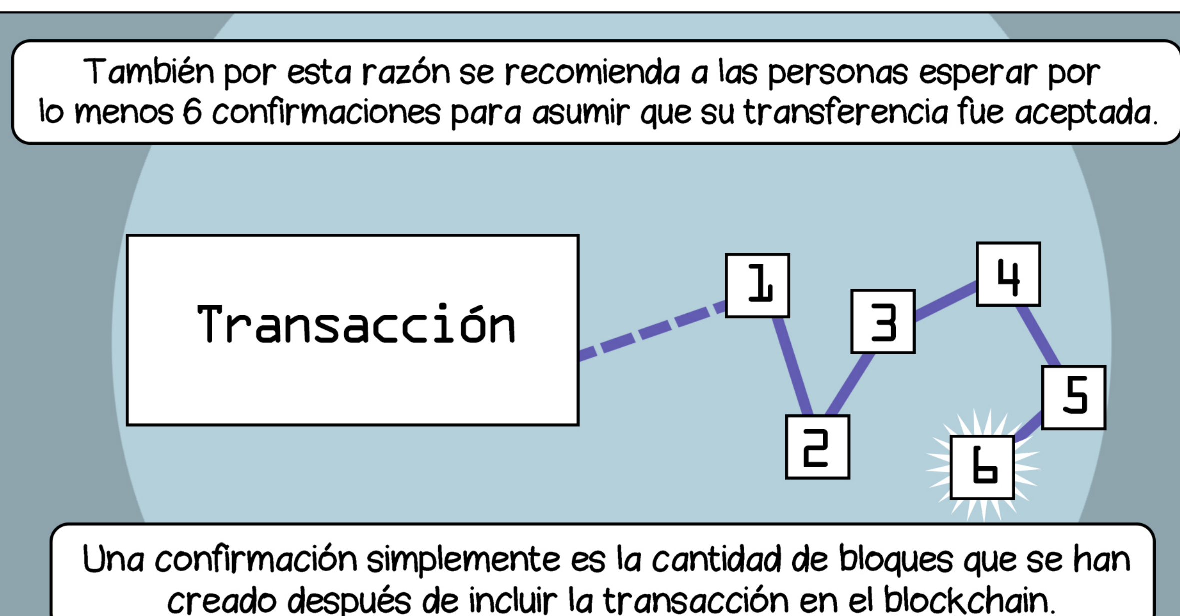
Las transacciones de la versión corta (desechada) que no estén presentes en la versión larga (oficial) volverán a estar pendientes...

Confirmadas - Pendientes
0 30

... Y las criptomonedas ganadas por los mineros de la versión desechada no serán válidas.

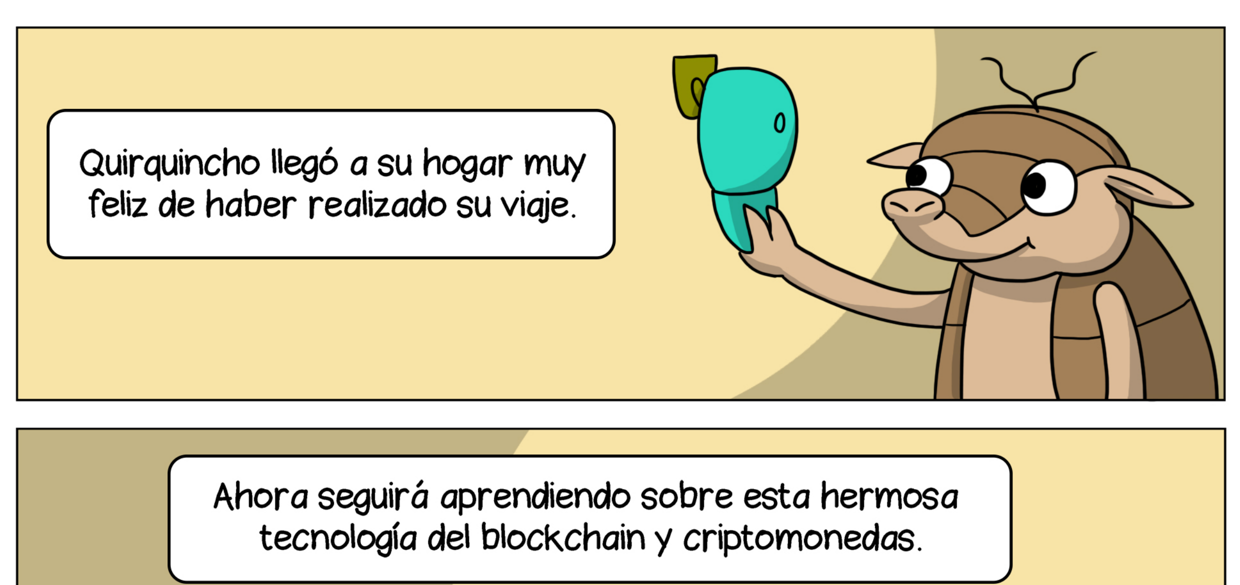






Al llegar a 6 bloques es muy probable que cualquier conflicto se haya resuelto y la transacción ha sido incluida en el blockchain oficial.

Transacción



Ahora seguirá aprendiendo sobre esta hermosa tecnología del blockchain y criptomonedas.

Ya que todavía hay mucho por descubrir.

Las Aventuras de

Quirquincho©



Las Aventuras de

Quirquincho©



www.chaucha.cl

